Intranet System For A Financial Services Corporation

BACKGROUND OF THE INVENTION

Field of the Invention:

The present invention relates to intranet systems; and more particularly, to an intranet system for a financial service corporation.

Description of the Prior Art:

An intranet is a private network that is contained within an enterprise. One purpose of an intranet is to share company information and computing resources among employees. Oftentimes, however, a company does not need to provide all available content to all users. In many instances, it is necessary to limit users to particular information, applications, functions and web pages. For instance, in the setting of a financial service corporation, it is costly to provide market data information that is accessed, at a cost, from an external service, e.g., Quotron by Reuters. Accordingly, there is a need in the art for an intranet system that can limit information, etc. that a user can access.

The presently available intranet systems available are also unmanageable as no mechanism exists for easy editing and updating of content. It, therefore, would also be advantageous for the content of an intranet system to be easily managed.

SUMMARY OF THE INVENTION

In accordance with the present invention, there is provided an intranet system for a financial services entity, comprising an interface application for accessing at least one internal data source and at least one external data source that a user is entitled to access; and an authentication system for determining which data sources a user is entitled to access, displaying the data sources on the interface application and setting a user preference profile. Advantageously, the system of the present invention provides timely

information to a user. Furthermore, the system may also allow content providers and administrators access through the same authentication processes as any other user.

The present invention also provides a system for providing financial information to end users in a network environment comprising an interface having means for selectively displaying information from an internal data source and an external data source; and means for controlling the display of the information; and an authentication system having means for determining a set of data sources that a user is entitled to selectively access and display; and means for setting user preferences for the user based on a stored user preference profile.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be more fully understood and further advantages will become apparent when reference is made to the following detailed description of the preferred embodiments of the invention and the accompanying drawings, in which:

FIG. 1 is a block diagram of an intranet system in accordance with the present invention;

FIG. 2 is a video screen display illustrating the intranet system login dialog;

FIG. 3 is a video screen display illustrating an interface application for a particular user;

FIG. 4 is a block diagram of a content management system;

FIG. 5 is a block diagram of an authentication system; and

FIGS. 6-8 are systems flow diagrams depicting operation of the authentication system.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

For convenience purposes, the following disclosure has been broken into parts as follows:

I. System

II. Operation

A. Overview

B. Interface Application

C. Content Management System

D. Authentication System Detail

I. System:

The present invention provides an intranet system for a financial services entity which is capable of selectively displaying information in accordance with a user's entitlement access. This is accomplished by a system comprising an interface application for accessing at least one internal data source and at least one external data source; and an authentication system for determining which data sources a user is entitled to access, displaying the data sources on the interface application and setting a user preference profile. The system of the present invention further utilizes a content management system for editing and updating data. This feature affords system users with updated, streamlined information, edited for relevance.

Referring now to the drawings, there is shown in FIG. 1 an intranet system 10 utilized in a network of users 20 such as found in a financial services entity or corporation. In this setting, system 10 may provide users 20 with a wide variety of information for such activities as client prospecting and consulting, presentation preparation, understanding compliance guidelines and regulations and determining available training. System 10 thus provides information on internal matters to the financial entity such as training, employee issues, corporate policy, products and services, as well as external matters relevant to the entity's business, e.g., market data.

A "user" for purposes of this disclosure refers to any person or entity that may access intranet system 10, e.g., information seeker(s) 21 such as employees, broker(s), content provider(s) 36 and administrator(s) 38. It should be recognized that "content providers" may take a variety of forms such as brokers, division heads, human resource representatives, investment analysts, and the like. Any person or entity within the preferred setting of a financial service entity having relevant information may be a content provider.

Intranet system 10 includes a memory 12, a central processing unit (CPU) 14, input output (I/O) 16, and bus 18. Memory 12 may comprise any known type of data storage and/or transmission media, including magnetic media, optical media, random access memory (RAM), read-only memory (ROM), a data object, etc. Moreover, memory 12 may reside at a single physical location, comprising one or more types of data storage, or be distributed across a plurality of physical systems in various forms, e.g., host servers. CPU 14 may likewise comprise a single processing unit, or be distributed across one or more processing units in one or more locations, for example, on a client and server. I/O 16 may comprise any known or hereafter developed input output device, including a network system, modem, keyboard, mouse, voice, monitor, printer, disk drives, etc. Bus 18 provides a communication link between the components in system 10 and likewise may comprise any type of transmission link, such as electrical, optical, radio, and the like. In addition, although not shown, additional components, such as cache memory and communication systems, may be incorporated into system 10.

Stored in memory 12 are components of intranet system 10 including control 19, authentication system 80, content management system 26 and interface application system 28. An internal data source 32 may also be included for storing data. In a preferred setting, data source 32 is at least one database 75-77, 33. Here, database 75-77, 33 provides a myriad of data obtained from internal servers such as information pertaining to funds, securities, market planning and analysis, human resources data, as well as any

other information which may be utilized in accordance with the dictates of the present invention. Data source 32 may be local and may comprise one or more storage devices, such as a magnetic disk drive or an optical disk drive. In another preferred embodiment, data source 32 comprises data distributed across a local area network (LAN), a wide area network (WAN) or a storage area network (SAN) (not shown). An external data source 34 is preferably provided through an external service provider server. External data source 34 may provide information not readily available to the financial service entity from internal sources, e.g., market data or news.

Intranet system 10 is linked to any number of users 20 via communication system 22 with wide area networks (WAN), local area networks (LAN), and other private networks or the Internet. Communication system 22 may also utilize conventional token ring connectivity, Ethernet, or other conventional communications standards. Where users 20 are connected to intranet system 10 via the Internet, connectivity is provided by conventional TCP/IP sockets-based protocol. In this instance, users 20 establish connectivity to intranet system 10 through web sites accessible over the Internet by a user 20 via an external Internet service provider. In this environment, all data is preferably encrypted, e.g., with 128-bit encryption techniques, to ensure account integrity will be maintained. Advantageously, system 10 provides an advanced technology platform with a stable, fast operating environment, easy accessibility and usability, and the flexibility of remote computing. In addition, system 10 may be linked to other outside systems as, for example, those described in the co-pending U.S. application entitled "Systems for Providing Financial Services" and "Browser Interface and Network Based Financial Service System."

Each user 20 preferably has a user system or workstation (not shown) that includes a CPU, a video display screen (VDS), and a communication system for communicating between the workstation and system 10. A user's system may also include a core of interface application, as will be described below. Through messaging technologies, other advanced technology

interfaces such as a personal digital assistant, advanced cellular technology, web-based television and the like may be utilized with system 10.

II. Operation:

A. Overview:

Operation of intranet system 10 is described relative to FIGS. 2-8. As is described, a user must be "authenticated" prior to access to any of the information contained in system 10. Authentication means user ability to access system 10 in accordance with predetermined entitlement and preference profiles. As illustrated in FIG. 2, once a user 20 interfaces with system 10, authentication system 80 provides a video display of a login 40. The login identification and password procedure allows user 20 to access intranet system 10 through communication network 22. Activation of authentication system 80 may be provided by specialized software resident on a user 20 workstation that connects to intranet system 10. Alternatively, a user 20 may activate authentication system 80 by accessing an authentication system web site of intranet system 10 via a conventional web browser such as Microsoft Internet Explorer®.

Login information is transmitted to a security function (part of authentication system 80) where a user 20 is authenticated. This provides for confirmation of a user's identity. Of course, a user will be denied access to the system where authentication does not occur. The security functionality described herein also represents a single point of security control for removing a user from the system. Preferably, the security function is resident in more than one host server of system 10 in order to provide load balancing and disaster recovery.

In addition, authentication system 80 interfaces with an entitlement profile to determine the type of access a user has in the system. Otherwise stated, authentication system 80 dictates the information that the user is allowed to access. Thus, users are authorized access to different information, applications and features resident in system 10. For example, the entitlements

accorded to a human resource representative would make them unable to access investor-related information. In addition, authentication system 80 also interfaces with a customized preference profile resident in system 10. The user preference profile comprises stored data relating to user customized interface(s), as for example, customized screen settings, viewed information and the like, allows a user to customize his or her interface application, e.g., settings, market data preferences, etc.

Advantageously, use of entitlement and preference profiles in accordance with the present invention allows a user to freely move between different locations and maintain access and preferences set at a user's own system or workstation, i.e., at their "home" office. That is to say, these features provide nomadic capabilities that allow a single sign-on procedure that can be utilized with any user system; sometimes known as "free-seating".

After authentication, control 19 of system 10 activates either content management system 26 or interface application system 28 depending on the identity of user 20.

B. Interface Application:

Interface application system 28 provides user 20 with an interface application in accordance with predetermined entitlements and preferences. One such interface application 42 as used by a financial broker is illustrated in FIG. 3. Interface application 42 is activated by control 19 when a successful logon has been attained.

Interface application 42 includes toolbar 44; menu 46 for presenting available information selections 45 and providing navigation therebetween; global function selections 48; and at least one view window 50, 51 for presenting information from at least one data source 32, 34.

Toolbar 44 may include standard browser features such as back, forward, stop, refresh/reload, home and print. Preferably, toolbar 44 includes favorites selection 52, Internet selection 54 and Exit selection 56. Internet selection 54 is provided only in the instance where the Internet is not the form

of access by user 20. Internet selection 54 allows a user 20 to access the Internet in order to search the World Wide Web via known search engines or access web sites through known URLs. General Internet access also allows a user 20 to communicate with system users and others via conventional e-mail packages such as provided by Microsoft Outlook®. Exit selection 56 allows a user to successfully logoff of system 10.

Menu 46 provides a list of feature selections 45 available to user 20. In accordance with the present invention, menu 46 depends on a user's entitlement level. Thus, feature selections 45 is likewise dependent on a user's entitlement level. As will be discussed later, authentication system 80 determines a user entitlement level and populates interface application 42 accordingly. The exemplary feature selections 45 shown for a financial broker-type user comprise at least one of a newsletter, market support, consultative process, operations/services, research, legal & compliance, divisions, employee information and training. Of course, any number of additional or fewer feature selections 45 may be utilized according to a user's needs.

Feature selections 45 are linked to data sources 32, 34 and communicate various features for display such as textual information, applications, special functions and web pages. Each feature selection 45 is preferably a hypertext link, the selection of which forces the activation and/or display of the selected feature in at least one view window 50 adjacent to menu 46. The data source 32, 34 accessed by each feature selection 45 depends on the location of the data. For instance, employee information may be located on internal data source 32, while market support may be located on an external data source 34. One example of a preferred external data source is a real-time market data source such as Quotron® by Reuters®. This data source provides up-to-the-minute market data for users. The ability to access external data source 34 affords system 10 a multitude of options without entity-wide effort.

After a feature selection 45 is made, user 20 may navigate within view window(s) 50, 51 to access further levels of information. In this way, a hierarchy of information may be created for organizational purposes.

As shown, more than one view window 50, 51 may be displayed at one time. This permits the selection of more than one feature selection 45 and thus, the simultaneous view of resultant information, applications, functions or web pages on split screens 50, 51, or other layout as known in the art. Each view window 50, 51 may include conventional scroll bars as necessary. In accordance with the particular user selection and dependent on system 10 configuration, the data is transmitted to the CPU of system 10 or is resident on the CPU of system 10. If transmitted, the CPU of a host server sends the data pertinent to the application selected to user 20 via network links or the Internet and is received by the user's CPU. Data from the CPU is uploaded into the RAM with the resultant graphical display on the user's VDS controlled by the contents of the RAM in a conventional manner. Whenever a new entry is selected, data is transmitted to the user in a similar manner. As previously mentioned, any number of information displays, applications, functions or web pages may run concurrently. These displays can be viewed in any format (e.g., split screen, cascade, minimized) selected by user 20.

Every interface application provides global function selections 48 regardless of the user's entitlement level or the chosen display. Preferably, global function selections 48 include search selection 58 for searching data sources 32, 34, site map selection 60 for viewing the hierarchy of data source 32, 34, who's who selection 62 for accessing a corporate directory, help selection 64 for accessing help features, feedback selection 66 for accessing an e-mail feed back form and forms selection 68 for accessing internal forms. Global function selections 48 also preferably includes a scratchpad application selector 70 for moving information between displays, applications and forms. When user 20 clicks on any of the global functions selection 48 buttons, the appropriate content replaces the current content in the display.

Advantageously, interface application 42 provides a seamless transition between the different features afforded by a user's entitlement level. Interface application 42 thus acts as a "controlled shell" of individualized features provided by system 10.

C. Content Management System:

Referring to FIG. 4, the content management system 26 of the present invention is illustrated. Content management system 26 is activated by control 19 (shown in FIG. 1) after authentication system 80 ascertains that user 20 is either a content provider 36 or an administrator 38. More specifically, content management system 26 includes administrator system 72 and content converter 74. Content management system 26 interfaces with internal data source 32 which preferably includes production database 75 for storing active content available to users 20, staging database 76 for storing content in development, and archive database 77 for storing old content. Internal data source 32 may also comprise other databases 33 as required.

Administrator system 72 is an access mechanism, i.e., a front-end, to internal data source 32 and allows comprehensive control of internal data source 32 content. Administration system 72 controls addition of new content, update of old content, updating of metadata, managing system-generated metadata regarding document status, managing content development and control processing, supporting archiving and deletion of content, managing the overall hierarchy of data source 32, managing attachments, administering appropriate hyperlinks and security, reviewing/previewing content in staging and the like. Thus, administrator system 72 controls data movement between production database 75, staging database 76 and archive database 77. Administrator system 72 allows access to the different databases by the directories/files of databases 75-77, 33 that are accessible to an administrative user 36, 38 through an explorer application (not shown), e.g., Microsoft Windows Explorer®. In conjunction with authentication system 80, administrator system 72 may also control user entitlement levels. As such,

content provider 36 access to system 10 may be controlled by the entitlements assigned by administrator 38. As illustrated in FIG. 4, content management system 26 also includes content converter 74. This feature transforms content submissions from content provider(s) 36 from a non-hypertext markup language (i.e., non-HTML format such as Word, Excel, PowerPoint, etc.) to HTML. Accordingly, content converter 74 allows system 10 to receive any typed content regardless of format.

In certain circumstances, a content provider 36 may be entitled to access content management system 26 and/or internal data source 32 directly. For instance, where information is time-sensitive, a content provider 36 may be given an entitlement level by authentication system 80 that allows for direct access to production database 75 and, hence, immediate posting of content.

D. Authentication System Detail:

Referring to FIGS. 5-8, authentication system 80 is shown in greater detail. Authentication system 80 allows a user 20 to access system 10 features in accordance with predetermined entitlements. For instance, brokers may be entitled to access the features shown on interface application 42 in FIG. 3. A human resource representative may be accorded access to most of the same features except market support and legal & compliance information.

Similarly, authentication system 80 determines access to content management system 26 for content provider(s) 36 or administrator(s) 38 and assigns the degree of access for these specific users. For example, a content provider may be allowed to submit content to a staging database but would have no other access. Another content provider may have access to staging database 76 and production database 75 for time-sensitive content posting. An administrator may have complete access to administrator system 72 in order to control content of internal data source 32, i.e., control data/content movement between production database 75, staging database 76, archive database 77 and/or other database(s) 33. As noted above, administrator system 72 may

also allow database access by the directories/files of the databases 75-77, 33 that are accessible to an administrative user 36, 38 through an explorer application (not shown), e.g., Microsoft Windows Explorer®.

For non-administrative users, interface application 42 displays the features available to a specific user as determined by their entitlement level. From this information, authentication system 80 builds the appropriate interface application. In one embodiment, a user entitlement level stored in an entitlement database(s) 33 includes a number of identifications or passwords for user 20, e.g., home wirecode, home branch group, external data source 34 server ID, and security ID. A particular user 20 system or workstation may also be limited in access and also include an entitlement level stored in an entitlement database(s) within system 10. In this instance, a customized user preference profile is stored in a database(s) 33 and contains customized settings, e.g., user's toolbar 44 settings, etc. A user's preference profile is used to build interface application 42 and provide the user with previously set preferences. In another embodiment, the entitlement and preference information is stored in the MAC function discussed below.

As shown in FIG. 5, authentication system 80 includes shim module 82, controller 84, logon-off control module 86, shell initialization module 88, interface launch module 90, password module 92 and MAC 93. Operation of authentication system 80 will be described relative to FIGS. 6-8. It is also noted that authentication system 80 is described relative to a system 10 having a preferred distributed server system. A single server may be utilized as well.

Referring to FIG. 6, in a first step S1, a user boots a user system or workstation (not shown), i.e., turns on or re-starts a workstation.

In step S2, a normal boot sequence is interrupted and shim module 82 is activated to direct operation to logon-off control system 86, i.e., standard workstation protocols (e.g., Winlogon) are interrupted. Logon-off control system passes through all requests for service to controller 84 and loads shell initialization module 88 and interface system launch module 90. In a preferred embodiment, shim module 82 replaces a Microsoft® graphical

identification and authentication dynamic link library (GINA dll) that operates with the Winlogon component of Microsoft® Windows NT® with a special system GINA dll that acts as controller 84.

As will become evident, controller 84 (sometimes through modules 82, 86, 88, 90, 92) governs a number of activities including retrieval of a user's preference profile; populating interface application 42; finding a user's entitlement level; retrieving numerous user identifications (e.g., home wirecode, home branch group, external data source 34 server ID, and security ID for use by shell initialization module 88); creating a local user directory based on a user's preference profile; storing user password(s) in a library for applications to retrieve; setting an access control list on a logging-in user's directory to provide full control; verifying and backing up user preference profiles; removing local preference profiles (excepting defaults, administrative and guest settings); and notifying a user of password expiration.

As one with ordinary skill in the art will recognize, when a user 20 accesses system 10 over the Internet, steps S1 and S2 are not required as the user system or workstation has already been booted. In this setting, when user 20 accesses a login web page of system 10, shim module 82 replaces the Microsoft® graphical identification and authentication dynamic link library (GINA dll) that operates with the Winlogon component of Microsoft® Windows NT® with a special system GINA dll that acts as controller 84. Logon-off control module 84 then passes through all requests for service to controller 84 and loads shell initialization module 88 and interface system launch module 90.

At step S3, controller 84 authenticates a user logging-on by activating password module 92. Password module 92 may access a special security server (not shown) to authenticate a user. Upon initialization of security server, a user will be presented with a dialog for input of a user name and password.

Controller 84 may also indicate that a password change is required, i.e., it is about to expire based on information from the security server. At

this time, a move/add/change (MAC) function 93 notifies the user that a password-reset operation has been performed and the password must be changed. The password may be changed in any conventional way of inputting a new password with a confirmation. MAC function 93 also updates a security function with new or revised user names, entitlements, social security functions, advisor identification number (where appropriate), identification for market data entitlements, and satellite branch identifiers (where appropriate), as well as an email alias and title. The MAC function is a single entry point to fully add or remove a user from all required security or distributed systems that support platform functionality. Additional details on the MAC functionality are provided in the copending U.S. application entitled "Browser Interface and Network Based Financial Service System," both of which are expressly incorporated herein by reference.

At step S4, controller 84 creates a local user directory, verifies that a user preference profile path for the user exists and backs up the user preference profile. A user preference profile may exist on a local user workstation server or another server within system 10, i.e., it may be local or remote. A user preference profile includes a number of directories and files of the user, also know as the user's registry, utilized by system 10 to access a user's information. If controller 84 cannot verify a path, authentication system 80 uses a default profile. If a registry fails to load, controller 84 may attempt to use a user's last known profile, which may be accessible from a profile back up. Creating a local user directory on a user's system or workstation includes mapping the directories of the system or workstation the user is using to the registry of directories and files for a user.

At step S5, after a user is authenticated, logon-off control 86 executes shell-initialization module 88 ("shell-init module").

At step S6, shell-init module 88 determines whether a previous logon did not proceed normally. If so, shell-init module 88 undoes the changes made during the last logon, i.e., it remembers user preference profile changes made during the previous logon.

At step S7, shell-init module 88 maps server names for user information to server IP address and port number. Where the user is connected to the system 10 via a network, this is accomplished by determining a physical wire code from the physical location of the user's local server; a user's home server wire code from the user preference profile (where necessary); and a user's parent server wire code (where necessary) by querying the entitlement data. A user "home" server is one located at a user's main office; a "parent" server is one to which a group of user home servers are connected, i.e., a division server. If the user is accessing system 10 via the Internet, the system recognizes the user as being at a remote site.

Next, turning to FIG. 7, at step S8, shell-init module 88 connects to an entitlement database which resides wither in database 33 or the MAC function. Access to user entitlement level is based on the user identity input at authentication. Shell-init module 88 attempts first to access the entitlement database to determine this information. If unable to do so, system 10 has a failover to a central server entitlement database (i.e., one to which a number of parent servers are connected and may include duplicate entitlement databases).

Next at step S9, shell-init module 88 retrieves a particular user's system or workstation entitlement level and the user's entitlement level. In particular, shell-init module 88 retrieves a list of user identifications for accessing particular data source 32, 34 features. These identifications are stored for use by interface application 42.

At step S10, shell-init module 88 logs-on to an appropriate server and retrieves entitlement data. Shell-init module 88 secures registry entries for interface application 42, attains a user control list of features and a batch file for interface system launch module 90, and a user's parent wire code (where appropriate).

Next at step S11, shell-init module 88 may map a user's system or workstation's local resource drives to a user's directories/files, i.e., distributed file system (DFS), by reading from the user's preferences and substituting

variables with wire codes, branch groups (where necessary) and user names as appropriate. DFS may be located in any of system 10's host server's component servers.

At step S12, shell-init module 88 activates interface system launch module 90, which runs throughout a user's session. Interface system launch module 90 builds menu 46, starts toolbar 44, and handles security ticket expiration, user log-off and user system or workstation restorations. With special regard to security ticket expiration, launch module 90 continually monitors a security time ticket and gives a warning to a user when time is about to expire. This is provided by querying password module 92 to determine what time allotment a user may have.

Next at step S13, launch module 90 applies the entitlement data to the local workstation registry, i.e., it removes the local preference profile of the workstation utilized by the user. Thereafter, launch module 90 signals controller 84 to start interface application 42.

At step S14, controller 84 starts interface application 42, and launch module 90 populates menu 46 with the user's entitled data source 32, 34 features, and starts toolbar 44 and any other ancillary processes. During this time, launch module 90 retrieves path names of executables to launch from the registry. For instance, external data source(s) 34 may require a user identification and password in order to access data stored therein. Some features execute and are monitored, some execute but are not monitored, and some execute at log-off. These are monitored by launch module 90 so appropriate action may be taken.

At step S15, shown in FIG. 8, launch module 90 activates interface application 42.

At step S16, the system is used to investigate information, learn about regulations and compliance, conduct various finance-related activities such as advising investors, or the like. This affords the user with timely, proactive financial advice as well as a variety of information about the finance service entity. Similarly, a user 20 can obtain information about a variety of aspects

of financial service entity, e.g., internal policies, holidays, employee matters, etc. Launch module 90 monitors a user's time versus a security ticket expiration and notifies a user when his or her time is about to expire. The notification may provide a user with the ability to extend the ticket, otherwise, the user will be forcibly logged-off.

At step S17, a user logs-off the system 10, at which time launch module 90 restores the user workstation registry entries that were in place prior to the user's sessions and clears the start menu. A log-off may be instigated by selecting Exit selection 56 of interface application 42.

At step S18, launch module 90 passes control back to standard workstation protocols, e.g., Winlogon, and controller 84 copies a user's preferences from local cache to the location from which it attained them as appropriate so a user's changes can be accessed the next time the user logs on.

The authentication system 80 thus described allows a user to access features, i.e., information, applications, functions and web pages, according to entitlement levels and provides a user preference profile for that user regardless of where a user is physically located. As such, the system 80 allows a user 20 to logon anywhere and have all of the features and preferences available as if they were at their own workstation.

Having thus described the invention in rather full detail, it will be recognized that such detail need not be strictly adhered to but that various changes and modifications may suggest themselves to one skilled in the art, all falling within the scope of the invention, as defined by the subjoined claims.